

BAB I PENDAHULUAN

1.1 Latar Belakang

Era digital yang semakin maju menjadikan kebutuhan akan perlindungan informasi sebagai hal yang sangat penting. Salah satu metode yang digunakan untuk menjaga kerahasiaan informasi adalah steganografi, yaitu sebuah metode yang bertujuan untuk mengamankan dan menyisipkan pesan ke dalam data digital salah satunya gambar, sehingga pesan tidak bisa dibaca oleh sembarang orang kecuali penerima yang dituju [1]. Berbeda dengan kriptografi yang mengamankan isi pesan, steganografi bertujuan untuk menyamarkan keberadaan pesan itu sendiri agar tidak terdeteksi [2].

Steganografi citra digital umumnya memanfaatkan domain spasial sebagai lokasi penyisipan data dengan cara memodifikasi nilai piksel langsung, seperti pada metode *Least Significant Bit* (LSB) [3]. Meskipun metode ini sederhana dan memiliki kapasitas penyisipan yang tinggi, pendekatan spasial cenderung kurang memiliki *imperceptibility* dan *robustness*, karena mudah terpengaruh oleh proses kompresi, *filtering*, atau serangan steganalisis [4]. Hal ini menyebabkan data rahasia rentan rusak atau terungkap apabila citra mengalami manipulasi.

Pendekatan berbasis domain frekuensi seperti *Discrete Wavelet Transform* (DWT) mulai dikembangkan sebagai solusi terhadap keterbatasan pada domain spasial. DWT mampu memecah citra menjadi empat *Sub-band*, yaitu LL, LH, HL, dan HH, yang merepresentasikan berbagai komponen frekuensi [5]. *Sub-band* HH, yang menyimpan detail frekuensi tinggi, dipilih sebagai lokasi penyisipan karena dapat dimodifikasi dengan dampak minimal terhadap tampilan visual keseluruhan citra, sehingga meningkatkan tingkat *Imperceptibility* [5].

Pendekatan steganografi modern sekarang mengadopsi teknik *deep learning* seperti *Generative Adversarial Network* (GAN) agar meningkatkan *Imperceptibility* dan *robustness* terhadap gangguan *noise* dan kompresi. GAN terdiri dari tiga jaringan, yaitu *generator* sebagai penyisip pesan rahasia, *discriminator* sebagai pendeteksi citra stego, dan *Extractor* untuk mengekstraksi pesan rahasia dari citra stego [6]. Melalui pelatihan secara *adversarial*, sistem ini mendorong *generator* menghasilkan citra stego yang sangat mirip dengan citra asli sehingga sulit dibedakan oleh pengamat maupun steganalisis [6].

Beberapa peneliti telah melakukan Penelitian terhadap steganografi menggunakan *Generative Adversarial Network* (GAN) dan *Discrete Wavelet Transform* (DWT). Penelitian yang dilakukan oleh Souvik Bhattacharyya [5] dalam jurnalnya berjudul “*A Robust Image Steganography using DWT Difference Modulation (DWTDM)*”, merancang sistem yang dapat menyembunyikan data

dalam gambar menggunakan modulasi perbedaan DWT. Penyisipan data dilakukan pada sub-band HL, LH, dan HH dengan melakukan dekomposisi satu level. Hasil penelitian menunjukkan bahwa metode DWTDM memiliki nilai PSNR sebesar 38.56 dan nilai SSIM sebesar 0.884.

Penelitian lain oleh Vida Yousefi Ramandi [7] dalam jurnalnya yang berjudul “*VidaGAN: Adaptive GAN for image steganography*”, merancang sistem yang dapat menyembunyikan data biner dalam gambar menggunakan GAN. Pada penelitian ini, diperkenalkan arsitektur baru yang terdiri dari *encoder*, *decoder*, dan kritikus untuk meningkatkan kapasitas penyembunyian dan akurasi. Pada penelitian ini digunakan dataset DIV2K untuk melatih dan menguji model. Hasil dari penelitian memperoleh nilai PSNR sebesar 38.56 dan nilai SSIM sebesar 0.884 untuk kedalaman bit 6.

Sementara itu, Ye Yao [8] dalam jurnal berjudul “*High Invisibility Image Steganography with Wavelet Transform and Generative Adversarial Network*” mengusulkan metode steganografi gambar dengan menggabungkan DWT dan GAN untuk meningkatkan keamanan dan ketidakterlihatan pesan tersembunyi. Citra cover ditransformasi ke domain DWT, dan data disisipkan pada sub-band LH, HL, dan HH. *Discriminator* dirancang untuk membandingkan citra secara *patch-to-patch* menggunakan LSGAN *loss*, meningkatkan deteksi terhadap *Stego image*. Hasil eksperimen ini memperoleh nilai PSNR sebesar 40.49 dan nilai SSIM sebesar 0.9834 untuk payload 3 bpp dengan data latih menggunakan dataset COCO.

Penelitian sebelumnya telah mencoba menggabungkan DWT dengan GAN untuk memanfaatkan keunggulan masing-masing. Namun, umumnya pendekatan tersebut menerapkan *discriminator* setelah proses *inverse* DWT (IDWT), yang berarti proses klasifikasi dilakukan terhadap citra stego secara utuh [8]. Strategi ini menyebabkan kompleksitas komputasi yang tinggi, karena jaringan perlu memproses seluruh citra, dan bukan hanya bagian yang dimodifikasi. Hal ini berdampak pada rendahnya efisiensi pemrosesan, terutama untuk aplikasi *real-time* atau perangkat dengan keterbatasan daya komputasi.

Penelitian ini mengusulkan metode steganografi citra berbasis DWT-GAN, di mana penyisipan data dilakukan secara spesifik pada *Sub-band* HH oleh *generator*, dan *discriminator* GAN langsung mengevaluasi *Sub-band* HH hasil penyisipan tanpa menunggu proses rekonstruksi citra penuh. Setelah proses *embedding* selesai, citra stego direkonstruksi menggunakan *inverse* DWT dari semua *Sub-band*, termasuk HH yang telah termodifikasi. Pendekatan ini diharapkan mampu meningkatkan *Imperceptibility*, *robustness*, dan efisiensi komputasi dibandingkan metode-metode sebelumnya.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah:

1. Bagaimana penerapan metode steganografi berbasis *Generative Adversarial Network* (GAN) pada *Sub-band* HH dalam domain *Discrete Wavelet Transform* (DWT) dapat meningkatkan *Imperceptibility*, *robustness*, dan efisiensi komputasi pada proses penyisipan data rahasia dalam citra digital?
2. Bagaimana pengaruh penerapan *discriminator* langsung pada *Sub-band* HH terhadap kinerja sistem dalam membedakan citra asli dan citra stego tanpa melalui proses *inverse* DWT secara keseluruhan?

1.3 Tujuan

Adapun tujuan dari penelitian ini adalah:

1. Mengimplementasikan sistem steganografi citra menggunakan metode DWT dan GAN yang menyisipkan data pada *Sub-band* HH.
2. Menganalisis pengaruh evaluasi langsung pada *Sub-band* HH oleh *discriminator* terhadap kualitas citra stego (*Imperceptibility*), ketahanan (*robustness*), dan efisiensi komputasi sistem.

1.4 Batasan Masalah

Adapun batasan masalah yang dibahas pada penelitian ini adalah:

1. Metode steganografi dilakukan pada domain frekuensi menggunakan *Discrete Wavelet Transform* (DWT), khususnya *Sub-band* HH.
2. *Discriminator* hanya melakukan evaluasi pada *Sub-band* HH tanpa mengolah hasil *inverse* DWT secara keseluruhan.
3. Data rahasia yang disisipkan berupa pesan teks.
4. Citra yang digunakan pada pengujian yaitu citra warna, citra *grayscale*, dan citra medis.
5. Penilaian performa sistem difokuskan pada parameter *Imperceptibility* (PSNR, SSIM).
6. Pengujian ketahanan (*robustness*) dilakukan pada model yang memiliki nilai BER paling rendah.

1.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah:

1. Memberikan kontribusi dalam pengembangan metode steganografi yang lebih efisien dan sulit terdeteksi melalui integrasi GAN dan DWT pada level *Sub-band*.
2. Menjadi referensi bagi penelitian selanjutnya dalam penerapan *deep learning* untuk keamanan informasi, khususnya pada sistem penyisipan data digital berbasis citra.

1.6 Sistematika Penulisan

Sistematika penulisan dari tugas akhir ini adalah :

BAB I PENDAHULUAN

Bab ini berisi uraian latar belakang penelitian, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang teori dasar yang mendukung dalam penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang penjelasan dan langkah-langkah mengenai penelitian yang dilakukan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi hasil data dan analisis dari penelitian.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran atas penelitian yang dilakukan.

